AO 106 (Rev. 04/10) Application for a Search Warrant (Modified: WAWD 10-26-18)

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* Information associated with Apple ID berhane_atakilte@hotmail.com that is stored at premises controlled by Apple	)	Case No. MJ20-248

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A, incorporated herein by reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
21 U.S.C. § 841	Distribution of Methamphetamine and Heroin
21 U.S.C. § 846	Conspiracy

The application is based on these facts:

✓ See Affidavit of Special Agent Shawna Mccann, continued on the attached sheet.

☐ Delayed notice of days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Pursuant to Fed. R. Crim. P. 4.1, this warrant is presented: ☑ by reliable electronic means; or: ☐ telephonically recorded.

Applicant's signature

Shawna Mccann, Special Agent

Printed name and title

○ The foregoing affidavit was sworn to before me and signed in my presence, or

◉ The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone.

Date: 05/14/2020

Judge's signature

City and state: Seattle, Washington

Mary Alice Theiler, United States Magistrate Judge

Printed name and title

USAO: 2019R01230

AFFIDAVIT OF SHAWNA MCCANN

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, SHAWNA MCCANN, a Special Agent with the Federal Bureau of Investigation, Seattle, Washington, having been duly sworn, state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been employed with the FBI since September, 2017. I am currently assigned to the Seattle Field Division where I am a member of the violent crime, gang, and Transnational Organized Crime – Western Hemisphere squad. As an FBI Special Agent, I have investigated a variety of drug-related crimes, including cases involving the introduction and possession of controlled substances and other contraband in a federal detention center. In this capacity, I investigate, *inter alia*, violations of Title 18, United States Code, Section 1791 (providing or possessing contraband in prison); Title 21, United States Code, Sections 841 and 846 (possession and distribution of controlled substances, and conspiracy thereof); and related offenses. I have received specialized training in the enforcement and investigation of drug-related crimes. I have received over 400 hours of classroom training including, but not limited to, drug identification, drug interdiction, smuggling, and the investigation of individuals and/or organizations involved in the illegal possession, possession for sale, sales, importation, smuggling, manufacturing, and trafficking of controlled substances.

2. During my career as a Special Agent, I have participated in narcotics investigations (*e.g.*, heroin, cocaine, marijuana, and methamphetamine) that have resulted in the arrest of individuals and the seizure of illicit narcotics and/or narcotics-related evidence and the forfeiture of narcotics-related assets. I have been involved in the service of federal and state search warrants as part of these investigations. I have encountered and have become familiar with various tools, methods, trends, paraphernalia, and related

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

articles utilized by various traffickers in their efforts to import, export, conceal, and distribute controlled substances. I am also familiar with the manner in which drug traffickers use telephones, often cellular telephones, to conduct their unlawful operations, and how they code their conversations to disguise their unlawful activities. I am also familiar with the various methods of packaging, delivering, transferring, and laundering drug proceeds. Additionally, through my training and experience, I can identify illegal drugs by sight, odor, and texture.

3. I have also worked on drug investigations involving the use of court-authorized wiretaps under Title III and monitoring of recorded prison phone calls. During these investigations, I have had the opportunity to monitor, listen to, and review transcripts and line sheets (prepared by linguists) documenting the content of hundreds of intercepted conversations involving the trafficking of cocaine, methamphetamine, heroin, and other narcotics, by persons who used some form of code to attempt to thwart detection by law enforcement. I have also interviewed defendants at the time of their arrest and have debriefed, spoken with, and/or interviewed numerous drug dealers or confidential sources at proffer and field interviews who were experienced in speaking in coded conversation over the telephone. From these interviews, and also from discussions with other experienced agents,[1] I have gained knowledge regarding the various methods, techniques, codes, and/or jargon used by drug traffickers in the course of their criminal activities, including their use of cellular telephones and other electronic means to facilitate communications while avoiding law enforcement scrutiny.

4. I have written affidavits in support of court-authorized federal warrants and orders in the Western District of Washington for Global Positioning Device ("GPS") tracking of telephones, Pen Register/Trap and Trace, and search warrants. Additionally, I

[1] When I use the term "agents" throughout this Complaint, I am referring to law enforcement personnel including, but not limited to, FBI agents, task force officers, Seattle Police Department sergeants, detectives, and officers, and federal detention center staff.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

have testified in grand jury proceedings, written investigative reports, and conducted and participated in numerous interviews of drug traffickers of various roles within drug organizations, which has provided me with a greater understanding of the methods by which drug trafficking organizations operate. I have also conducted and participated in numerous interviews of inmate victims, inmate witnesses, and inmate subjects, which have provided me with a greater understanding of drug-related offenses committed in federal detention centers.

5. The facts set forth in this Affidavit are based on my personal knowledge; knowledge obtained from others during my participation in this investigation, including other law enforcement officers; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the Application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

PURPOSE OF AFFIDAVIT

6. This Affidavit is made in support of an Application for a search warrant pursuant to Title 18, United States Code, Sections 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) for information associated with an iCloud account that is stored at premises controlled by Apple Inc. ("Apple"), located at One Apple Park Way in Cupertino, California, to require Apple to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B, pertaining to the following Apple ID, further described in Attachment A:

> Apple ID: berhane_atakilte@hotmail.com associated with DSID: 16568146691 (the "SUBJECT ACCOUNT").

Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

7. As discussed herein, there is probable cause to believe that the SUBJECT ACCOUNT contains evidence of providing drug and other contraband in a federal detention center and a conspiracy thereof, all in violation of violations of Title 18, United States Code, Section 1791 (providing or possessing contraband in prison); Title 21, United States Code, Sections 841 and 846 (possession and distribution of controlled substances, and conspiracy thereof); and related offenses. As such, there is probable cause to search the information described in Attachment A for evidence, instrumentalities, or contraband of these crimes, as described in Attachment B. Obtaining the information sought in this Affidavit is necessary to further the investigation into these offenses.

JURISDICTION

8. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that – has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

KNOWLEDGE BASED ON TRAINING AND EXPERIENCE

47. I have knowledge about iCloud based on my own training and experience, other investigations I have worked on, consulting with other agents, research on publicly available websites for Apple, and Department of Justice materials that document the services that these companies provide and what data they retain.

48. Based upon my training, experience, and conversations with other experienced officers and agents, I know that:

a. Drug traffickers use cellular telephones as tools or instrumentalities in committing their criminal activities. They use them to maintain contact with their suppliers, distributors, and customers. They prefer cellular telephones because, first, they can be purchased without the location and personal information that land lines require. Second, they can be easily carried to permit the user maximum flexibility in meeting associates, avoiding police surveillance, and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

traveling to obtain or distribute drugs. Third, they can be passed between members of a drug conspiracy to allow substitution when one member leaves the area temporarily. Since cellular phone use became widespread, every drug dealer I have contacted has used one or more cellular telephone for his or her drug business.

b. I also know that it is common for drug traffickers to retain in their possession phones that they previously used, but have discontinued actively using, for their drug trafficking business.

c. Based on my training and experience, the data maintained in a cellular telephone used by a drug dealer is evidence of a crime or crimes. This includes the assigned number to the cellular telephone (known as the mobile directory number or MDN), and the identifying telephone serial number (Electronic Serial Number or ESN), (Mobile Identification Number or MIN), (International Mobile Subscriber Identity or IMSI), or (International Mobile Equipment Identity, or IMEI) are important evidence because they reveal the service provider, allow us to obtain subscriber information, and uniquely identify the telephone. This information can be used to obtain toll records, to identify contacts by this telephone with other cellular telephones used by co-conspirators, to identify other telephones used by the same subscriber or purchased as a part of a package, and to confirm if the telephone was contacted by a cooperating source or was intercepted on a wiretap here or in another district.

d. Persons involved in drug trafficking will obtain and distribute the drugs on a regular basis, much as a distributor of a legal commodity would purchase stock for sale. Similarly, drug traffickers will maintain an "inventory," of drugs, which will fluctuate in volume depending upon the demand for and the available supply of the documents/goods.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

e. Drug traffickers' methods of storing and distributing their illegal merchandise include hiding them on their person or in their residences, vehicles, businesses, and storage units.

f. In my experience, and in the experience of other law enforcement officers I have consulted with, drug traffickers go to great lengths to conceal their illegal business operations. Traffickers utilize many methods to hide or conceal drug-related activity, other illegal merchandise, and/or currency related to their illegal operations, including hidden on their person, concealed in shopping, duffel, and tote bags, and hidden in compartments in vehicles.

BACKGROUND KNOWLEDGE OF APPLE

49. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

50. Apple provides a variety of services that can be accessed from Apple devices, such as an iPhone, or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices, including iPhones, to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps. iCloud can be utilized to transfer data from an old device to a new device, including data derived from device backups and third-party applications.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

f. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

51. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

52. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

53. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

54. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

55. The following definitions are provided to explain some of the terms used specific to this investigation. These definitions are provided here in part only and do not purport to be all possible objective or subjective definitions of such terms:

a. **Internet**: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

b. **IP Address**: An Internet Protocol ("IP") address is a unique numeric address used by devices, such as computers, on the Internet. Every device attached to the Internet must be assigned an IP address so that Internet traffic sent from and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

directed to that device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses.

c. **Apple iMessage and FaceTime**: Apple's iMessage and FaceTime services allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video or audio calls.

d. **Apple ID**: Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. Apple uses a unique Destination Signaling Identifier ("DSID") to identify a user's Apple ID.

e. **Virtual Private Network ("VPN")**: A VPN connection is a means of connecting to a private network over a public network such as the Internet. A VPN is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption. VPN's are also frequently used by people who wish to circumvent geographic IP limitations and censorship, and to connect to proxy servers for the purpose of obfuscating the source of an internet connection or transmission.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

STATEMENT OF PROBABLE CAUSE

18. As discussed in more detail below, HABEN SEBHATU, an inmate at the Sea-Tac Federal Detention Center ("FDC"), conspired with other individuals to introduce controlled substances and other contraband into the FDC on December 16, 2019. Inmate SEBHATU and ATAKILTE BERHANE, using a cell phone assigned the phone number 206-454-0193 (hereinafter, "TT1"), planned to take advantage of the FDC's visiting hours to stash controlled substances and a contraband cellular phone in a trash can in the facility's lobby bathroom, where they would later be retrieved by inmate MIMS GRAY, working on the maintenance crew. On December 16, 2019, technicians with the FDC's Special Investigative Services ("SIS") found controlled substances, including methamphetamine and heroin, and a cell phone concealed in a trash can in the FDC lobby bathroom.

Plan to Introduce Controlled Substances into the FDC

19. On or about December 14, 2019, an SIS Technician at the FDC reported that an inmate had discussed a plan to introduce a cell phone and other contraband into the facility during recorded prison phone calls between the inmate and an individual outside of the FDC.

20. On or about December 15, 2019, I spoke with an SIS Technician at the FDC and was advised that inmate SEBHATU had used another inmate's account[2] to make several phone calls to TT1 between December 9, 2019 and December 13, 2019.[3]

---

[2] Through a review of video surveillance, SIS Technicians at the FDC determined that the other inmate handed the phone off to inmate SEBHATU during the times that SEBHATU spoke with BERHANE from December 9, 2019 to December 13, 2019. Inmate SEBHATU also said his first name during the recorded prison calls on two occasion.

[3] I was advised by an SIS Technician at the FDC that TT1 was listed on this other inmate's contact list, used by inmate SEBHATU, as being associated with the name "Matt J." I know based on my training and experience that inmates create their phone and email contact lists, that these contact names are not verified by FDC or other Bureau of Prisons staff, and that inmates often list false names for contacts to conceal their contacts' true identities from law enforcement.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

During these recorded phone calls, inmate SEBHATU and the male user of phone number TT1, later identified as BERHANE, formulated the following plan to introduce a cell phone and drug contraband to the FDC:

> BERHANE confirmed that he procured a cell phone and other contraband to smuggle into FDC for inmate SEBHATU. BERHANE did not want to perform the actual introduction of contraband into the FDC himself, but he agreed to drive an unknown male referred to as "K2" to the prison to facilitate the introduction of contraband. Inmate SEBHATU and BERHANE planned that, during visitation hours on Monday, December 16, 2019 between 7:00 p.m. and 8:00 p.m., K2 would enter the front lobby of the FDC and sit among the other visitors. K2 would have the cell phone and other contraband concealed inside a bag, with the contraband wrapped in plastic wrap. K2 would go to the second bathroom in the FDC's front lobby and hide the bag containing the contraband in the trash can of the bathroom. K2 would then tell FDC staff an excuse, such as having forgotten his ID, to exit the front lobby and not return. Once the contraband was stashed in the trash in the front lobby bathroom, a male inmate who works on the maintenance crew and has access to clean that bathroom, later identified as inmate GRAY, would retrieve the contraband on behalf of inmate SEBHATU.[4]

[4] During the recorded prison calls between inmate SEBHATU and BERHANE, both parties converse in a mix of English and Tigrinya dialect, of East African origin. A linguist fluent in English and Tigrinya created a summary translation of the recorded prison phone calls, which agents have reviewed. Prior to the linguist's summary, agents had been able to determine the details of the plan to introduce contraband into the FDC based on the context of the conversations, the English portions of the conversations, and the use of common code words and language used frequently by other inmates, including those of East African descent, which are known to me and the agents with whom I consulted during this investigation. Prior to the linguist's summary of the recorded prison phone calls, agents believed the introduction of contraband was planned to occur between approximately 3:00 p.m. and 5:00 p.m. on December 16, 2019. The linguist's summary, however, indicates that the planned introduction was scheduled to take place between 7:00 p.m. and 8:00 p.m. on December 16, 2019.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

21. During these recorded prison calls between inmate SEBHATU and BERHANE, inmate SEBHATU referred to BERHANE by his first name. SEBHATU and BERHANE discussed bringing a niece's birthday party present to the FDC. Based on my training and experience, and the training and experience of other agents with whom I have consulted, I know that a "birthday present" is a common term used by inmates to refer to drug contraband intended to be smuggled into prison facilities. During these recorded prison calls, BERHANE talked about not knowing some of the concealed substances that he procured for inmate SEBHATU, and inmate SEBHATU allowed BERHANE to partially open some of the packaging for those substances. Inmate SEBHATU also instructed BERHANE on how to wrap and tie the contraband package.

22. During these recorded prison calls between inmate SEBHATU and BERHANE, inmate SEBHATU made statements to BERHANE that appear to instruct BERHANE to procure a black android cell phone, model J2 or equivalent, fully charge the cell phone, and then turn the volume and other sound mechanism on the phone off before attempting to smuggle it into the FDC. Inmate SEBHATU instructed BERHANE not to buy or activate the contraband cell phone and get someone else to buy and activate the contraband cell phone because BERHANE was under inmate SEBHATU's inmate contact list. Later in these calls, BERHANE confirmed that he, through another individual, had obtained a cell phone for inmate SEBHATU.

23. During these recorded prison calls between inmate SEBHATU and BERHANE, inmate SEBHATU also stated that the inmate on the inside who would retrieve the contraband from the lobby bathroom trash, later identified as inmate GRAY, is a big person who likes talking. Inmate SEBHATU told BERHANE that this inmate would receive $400 to $500 for assisting in the plan to introduce controlled substances and other contraband into the FDC.

24. On or about December 15, 2019, inmate MIMS GRAY received a Western Union wire money transfer in the amount of $500 from an individual outside the FDC, Z.K.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Introduction of Contraband into the FDC on December 16, 2019

25. Based on a review of the recorded phone calls, agents believed that BERHANE and K2 would attempt to introduce controlled substances and a contraband cellular phone into the FDC in the afternoon of December 16, 2019. On that day, agents conducted surveillance in the parking lot and front lobby of the FDC from approximately 1:50 p.m. to 5:00 p.m. At approximately 1:40 p.m., agents inspected the trash can in the second bathroom of the front lobby of the FDC and observed some trash, including used paper towels, but did not observe or locate any contraband at that time. At approximately 4:51 p.m., an agent inspected the trash can in the second bathroom of the front lobby of the FDC again and observed some trash, including used paper towels, but did not observe or locate any contraband at that time.

26. After approximately 5:00 p.m. on December 16, 2019, inmate SEBHATU made two recorded calls to BERHANE and spoke with BERHANE and a female I.K. SEBHATU was advised that K2 was not responding to anyone and had apparently backed out of introducing the contraband into the FDC. Inmate SEBHATU tried to persuade BERHANE and I.K. to conduct the introduction of contraband himself and herself, respectively.

27. Investigators later reviewed the video surveillance footage from the FDC and discovered that, at approximately 7:26 p.m., a white pickup truck entered the FDC parking lot and parked in the visitor parking area. An unidentified female exited the driver's seat of the white pickup truck and walked to the front lobby of the FDC at approximately 7:44 p.m. The unidentified female looked towards the direction of the bathrooms immediately upon entering the FDC lobby and then attempted to access the first bathroom in the lobby (which is for staff use only and is kept locked). The unidentified female then spoke to the FDC staff person working the front lobby and subsequently walked towards and went inside the second bathroom in the lobby at approximately 7:46 p.m. At approximately 7:49 p.m., the unidentified female exited the bathroom and departed the FDC without attempting to visit any inmate. The unidentified

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

female entered the driver's seat of the white pickup truck and departed the FDC at approximately 7:53 p.m.

28. At approximately 10:31 p.m., while conducting a physical search of the second bathroom in the front lobby of the FDC, SIS Technicians discovered the following controlled substances and contraband items in a trash can in the bathroom, concealed in a McDonald's bag and wrapped in plastic wrap:

a. One black LG cell phone, model LM-X320PM, MEID-D number 089 713 128 000 602 505;

b. 58 Suboxone-type strips;

c. 2 bags (10 grams) of suspected heroin, which field tested positive for the presence of heroin;

d. 2 bags (14 grams) of suspected methamphetamine, which field tested positive for the presence of methamphetamine; and

e. 1 bag (11 grams) of a green leafy substance suspected to be K2/Spice, which field tested positive for the presence of synthetic narcotics.

29. The recovery of the package from the bathroom in the front lobby of the FDC closely matched the plan to introduce controlled substances and a contraband cellular phone discussed by inmate SEBHATU and BERHANE during the recorded prison phone calls, including the date and time of the planned introduction of contraband and the contents of the package.

30. Shortly after the recovery of the contraband on December 16, 2019, SIS Technicians created a decoy contraband package, placed the decoy contraband package back into the McDonald's bag, and placed the McDonald's bag back into the trash can of the front lobby bathroom of FDC. At approximately 10:55 p.m., inmate MIMS GRAY, who works on the maintenance crew and has access to the FDC front lobby for cleaning purposes, entered the front lobby of the FDC and began his work duties. At approximately 11:01 p.m., inmate GRAY entered the front lobby visitor bathroom. At approximately 11:08 p.m., inmate GRAY entered the secure side of the FDC front lobby.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

A search of GRAY's person was conducted by SIS Technicians, which did not locate any contraband. A search of the trash GRAY had collected revealed that GRAY had removed the decoy contraband package from the McDonald's bag and placed it into the trash bag he was using to collect trash.

31. From December 9, 2019 to December 16, 2019 inmates GRAY and SEBHATU were housed in the same unit at the FDC, in cells that are near each other.

Identification of ATAKILTE BERHANE as the User of TT1

32. Agents subpoenaed subscriber information and toll records for TT1 with service provided by T-Mobile, which was subscribed to BERHANE with a subscriber address of 1105 E Fir St Unit 613, Seattle, Washington 98122.

33. Agents reviewed the inmate visitor list for SEBHATU and noted that SEBHATU had listed "ATAKILTE BERHANE" as his "COUSIN" with an address of "1105 E FIR ST #613 SEATTLE WA 98122." Agents reviewed the inmate contact list for SEBHATU and noted that SEBHATU had listed BERHANE as his "Friend" with an address of "1105 E FIR ST SEATTLE WA 98122;" a second address of "154 HOLLY PARK DR S SEATTLE Washington 98118;" an active contact phone number as of December 4, 2019 of 206-853-3207; and an inactive phone number as of March 7, 2019 of TT1.

34. Agents reviewed the FDC money transaction list for inmate SEBHATU and noted that BERHANE sent money to inmate SEBHATU through Western Union Money Gram, which was received by FDC on November 14, 2019 at 5:03 a.m. in the amount of $50.00 and again on November 14, 2019 at 4:03 p.m. in the amount of $33.00. Both Money Grams from BERHANE to inmate SEBHATU listed BERHANE's phone number as TT1 and an address of 1105 E Fir St., Seattle, WA 98122.

35. Agents issued a subpoena to Western Union for records associated with the two Money Gram transactions initiated by ATAKILTE BERHANE to inmate SEBHATU, and that were received by the FDC on November 14, 2019. According to responsive documents, the sender of both transactions listed himself as BERHANE and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

used a date of birth in 1993. Agents conducted a search of law enforcement databases and Washington Department of Licensing and identified BERHANE's date of birth as the same date listed on the Money Gram records. For the transaction of $33.00, BERHANE initiated the transaction on November 14, 2019 at approximately 4:14 p.m. and used a device with an IP Address of 172.58.45.115. Agents conducted open source research on IP Address of 172.58.45.115 and identified the Internet Service Provider as T-Mobile USA, Inc. Agents believe BERHANE may have used TT1 (service provided by T-Mobile) to conduct the $33.00 money transfer to inmate SEBHATU based on the corresponding T-Mobile IP Address attached to the money transfer. For both transactions, BERHANE listed his email address as Berhane_Atakilte@hotmail.com (the same email address is associated with the SUBJECT ACCOUNT).

36. In January 2020, Seattle Housing Authority provided me with the lease documents for 1105 E Fir St Unit 613, Seattle, Washington 98122, which showed that S.G. was the only listed and authorized tenant of the unit. An emergency contact form filled out by S.G. listed BERHANE as S.G's emergency contact with a relationship of "Son" and TT1 as BERHANE's phone number.

Search of BERHANE's Residence and Seizure of TT1 (an iPhone)

37. On February 18, 2020, the Honorable Mary Alice Theiler, United States Magistrate Judge for the Western District of Washington, signed a search warrant for BERHANE's residence, a unit in the Columbia City Station Apartments, and a search warrant for BERHANE's person.

38. On February 19, 2020 at approximately 6:00 a.m., agents executed these search warrants. BERHANE was located in the apartment and removed to the hallway. Pursuant to the warrant, agents searched BERHANE's person and located a black iPhone in BERHANE's pocket. While standing next to the iPhone taken from BERHANE's pocket, I dialed phone number 206-454-0193 (TT1) from my FBI issued cell phone. I observed the iPhone that was taken from BERHANE's pocket light up and indicate the phone was receiving a call.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

39. Pursuant to the warrant, agents searched the one-bedroom apartment and in the bedroom found documents linking BERHANE to the FDC and inmate SEBHATU, including a blank BOP visitor's form and two envelopes addressed to BERHANE from SEBHATU at the Boonville Correctional Center in Missouri.[5] Agents also located an LG cellular phone under the pillow on the bed. This cell phone is believed to have also been used by ATAKILTE BERHANE based on the cell phone's location in close proximity to other clothing and personal items of ATAKILITE BERHANE in the bedroom.

40. Agents placed BERHANE under arrest, advised BERHANE of the charge against him, and read BERHANE his *Miranda* rights from the FBI Advice of Rights form. BERHANE acknowledged that he understood his rights and stated that he did not wish to speak with agents. Agents did not ask him any further questions.

BERHANE's Use of the SUBJECT ACCOUNT via TT1 (an iPhone)

41. Based on my training and experience, and information obtained from Apple's website, a user can create an Apple ID by providing Apple with an email address, among other identifiers. Once provided, Apple will send a verification email to confirm that the email address is valid and can be accessed by the user. After the email is verified, an Apple ID is created, with the user's email address serving as the username for that Apple ID. Once an Apple ID is created, it can be used to send iMessages to or initiate FaceTime audio calls with other Apple subscribers. When an iMessage is sent, the recipient will receive not only the text of the message but also the email address associated with the Apple ID and any photograph that the sender has selected for that Apple ID. After an Apple ID is created, a user can add additional email addresses to his or her account. Once verified, the user can send iMessages or initiate FaceTime audio calls with other Apple subscribers using one of these addresses. This new email address

[5] SEBHATU is at the FDC serving his sentence on a conviction out of the Eastern District of Missouri.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

will appear as the sender's username when a recipient views an iMessage or receives a FaceTime audio call.

42. In April 2020, agents obtained information from Apple in response to a subpoena concerning the SUBJECT ACCOUNT**,** which showed the following information:

> Apple ID: berhane_atakilte@hotmail.com is associated with iCloud account DSID: 16568146691, created on March 25, 2019, with a subscriber name of "Atakilte Berhane" a subscriber address of "1105 E Fir st apt 613, Seattle, Washington," a subscriber daytime phone number of TT1, and a FaceTime and iMessage phone number of TT1.

43. The SUBJECT ACCOUNT has been linked to three devices: (1) an iPhone XS, serial number G0NXN653KPFQ, registered on March 26, 2019; (2) an iPhone XS, serial number GR4YX0H7KPFQ, registered on July 24, 2019; and (3) an iPhone XS, serial number GR4ZV0RAKPFQ, registered on March 3, 2020. All three of these cell phones are registered to "Atakilte Berhane" at "1105 E Fir St Apt 613, Seattle, Washington," and have TT1 as the phone number. Based on my training and experience, I know that Apple devices, including iPhones, have text message and email capabilities that allow the user to communicate with other individuals and Apple devices, and if the user has turned on iCloud settings, these emails, text messages, other communications, contacts, notes, and photographs can be stored and/or backed-up to the user's iCloud account.

44. As set forth above, ATAKILTE BERHANE used TT1 to conduct and facilitate a conspiracy to traffic narcotics and introduce narcotics into the FDC. Through TT1, ATAKILTE BERHANE may have accessed and used the SUBJECT ACCOUNT (his iCloud account), including Bookmarks, Contacts, iCloud Backup, iCloud Drive[6],

---

[6] According to Apple's website, iCloud Drive allows users to securely access documents from an iPhone, computer, or other Apple device, enabling users to edit and share documents across multiple devices.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

iCloud Photos, Messages in iCloud, and Notes. According to Apple records, BERHANE has activated the backup and storage of Bookmarks, Contacts, iCloud Backup, iCloud Drive, iCloud Photos, Messages in iCloud, and Notes to his iCloud accounts. Therefore, BERHANE's text messages, including text messages between BERHANE and other co-conspirators, contacts, iCloud backup and drive, photos, and notes are likely to be stored in the SUBJECT ACCOUNT.

45. In my training and experience, evidence related to criminal activity of the kind described above may be found in the files and records created, sent, and/or received on an Apple cell phone device and backed up to the user's corresponding iCloud account. In my training and experience, I also know that drug traffickers almost always use computers, smart phones, tablets, or other digital devices to conduct, facilitate, and further their criminal activities and enterprise.

46. In order to determine the scope and extent of the conspiracy described herein, agents seek records and information from Apple related to the SUBJECT ACCOUNT. As set forth herein, there is probable cause to believe that information contained in the SUBJECT ACCOUNT could reveal the identities of other members of the conspiracy. For example, co-conspirators could be ascertained by reviewing pictures stored in the iCloud Photo Library of the SUBJECT ACCOUNT. Similarly, co-conspirators could be ascertained by reviewing the Contacts, iMessages, and Notes stored in the SUBJECT ACCOUNT.

47. Additionally, there is probable cause to believe that information contained in the SUBJECT ACCOUNT will reveal BERHANE's use of the SUBJECT ACCOUNT and TT1 to conduct, facilitate, and further drug trafficking activities and other evidence of the drug trafficking crimes under investigation. For example, the SUBJECT ACCOUNT's iCloud Photo Library could contain photographs of narcotics and packaging, vehicles and other instrumentalities used by conspirators to traffic narcotics, and proceeds of narcotics transactions. Based on my training and experience, I know that drug traffickers take, or cause to be taken, photographs or videos of themselves, their

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

associates, their property, narcotics, and proceeds from narcotics transactions as a means of boasting about their enterprise and as a means of proving to customers and/or suppliers that the drug trafficker has the quantity and quality of narcotics and/or money on-hand. These photographs and videos are frequently taken, sent/received, and/or stored in the drug trafficker's cell phone devices.

48. iMessages stored in the SUBJECT ACCOUNT could contain information related to the dates, locations, dealers, and purchasers of narcotics transactions, and the type, quantity, quality, and pricing of narcotics being sold. Based on my training and experience, I know that drug traffickers utilize cell phones, text messages, and/or email devices for ready access to their clientele for the purpose of coordinating narcotics transactions, and to store customer and supplier names and contact information.

49. Notes and iCloud Drive stored in the SUBJECT ACCOUNT could contain information related to the dates, locations, dealers, and purchasers of narcotics transactions, and the type, quantity, quality, and pricing of narcotics being sold. Based on my training and experience, I know that drug traffickers often maintain records relating to the ordering, sale, and distribution of drugs and/or other goods and the outstanding debts and collections from purchasers, including but not limited to, electronically stored, computerized, or hand-written books, records, receipts, diaries, notes, ledgers, cashier's checks, money orders and other papers.

50. Other information connected to the SUBJECT ACCOUNT may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal additional services used by the user and corresponding user names, including app-based encrypted messaging platforms such as WhatsApp and Signal and app-based money transfer platforms including CashApp and Venmo. In addition, emails, instant messages, and notes can lead to the identification of members of the conspiracy and evidence and instrumentalities of the drug trafficking activity under investigation.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

PRIOR APPLICATIONS

51. On December 23, 2019, the Honorable Michelle L. Peterson, United States Magistrate Judge for the Western District of Washington, signed a search warrant for the contents of the LG contraband cell phone recovered on December 16, 2019, the search of which produced no data of evidentiary value.

52. On January 9, 2020, the Honorable Brian A. Tsuchida, Chief United States Magistrate Judge for the Western District of Washington, signed a search warrant for historical cell site data for TT1, a tracking warrant for real-time GPS location data for TT1, and a pen register and trap and trace order for TT1.

53. On February 3, 2020, the Honorable Mary Alice Theiler, United States Magistrate Judge for the Western District of Washington, signed a search warrant for the use of a cell-site simulator to locate TT1.

54. On February 18, 2020, the Honorable Mary Alice Theiler, United States Magistrate Judge for the Western District of Washington, signed search warrants authorizing the search of BERHANE's residence and person for evidence of the conspiracy to smuggle controlled substances into the FDC. TT1 and the SUBJECT DEVICE were found during the search, and BERHANE was arrested and charged by Complaint for conspiracy to distribute methamphetamine and heroin, in violation of Title 21, United States Code, Sections 841(a)(1) and (b)(1)(C), and 846.

55. On February 26, 2020, the Honorable Mary Alice Theiler, United States Magistrate Judge for the Western District of Washington, signed a search warrant for the contents of TT1 seized from BERHANE's person. Agents executed the search warrant later on February 26, 2020 and attempted to extract data from TT1 but were unsuccessful due to password protection on TT1. In March 2020, agents conducted another attempt to extract data from TT1 using a different technology method but were only able to extract a small amount of data due to additional security features on TT1. Agents are submitting TT1 to FBI Headquarters where one additional extraction method will be attempted on TT1; however, agents have been advised this method could take years to complete.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

56. On April 22, 2020, the Honorable Brian A. Tsuchida, Chief United States Magistrate Judge for the Western District of Washington, signed a search warrant signed a search warrant for the contents of the LG model cell phone seized from BERHANE's residence. Agents executed the search warrant on April 29, 2020 and attempted to extract data from this cell phone but were unsuccessful due to password protection on the device. Agents are submitting this device to FBI Headquarters where one additional extraction method will be attempted; however, agents have been advised this method could take several months to complete and may not be able to successfully bypass the security features on this cell phone.

OTHER INVESTIGATIVE TECHNIQUES

57. Agents have attempted to locate evidence of the conspiracy to traffic narcotics and introduce narcotics into the FDC by conducting searches of both cell phone devices believed to have been used by BERHANE, including TT1 and an LG device, the contraband cell phone introduced into the FDC on December 16, 2019 along with the narcotics. Agents have had limited success with these cell phone searches. As set forth above, agents have been unable to bypass security features on BERHANE's two cell phone devices, including TT1. Agents were able to successfully search and download data stored on the contraband cell phone introduced with the narcotics on December 16, 2019 because this cell phone was not password protected; however, this cell phone had very little data stored on it.

58. The information sought by agents through this Affidavit and Application for a search warrant to Apple regarding the SUBJECT ACCOUNT believed to be used by ATAKILTE BERHANE to conduct, facilitate, and further drug trafficking activities and the conspiracy will assist agents with identifying the means, methods, instrumentalities, tools, and additional co-conspirators, connected to the conspiracy, specifically by enabling agents to review contact lists, text messages, photos, notes, and other information that was created, sent, received and/or stored by ATAKILTE BERHANE using the SUBJECT ACCOUNT and TT1, including data that agents have been unable to

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

access to date through the direct search of the TT1 iPhone device due to security features on the device.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

59. Pursuant to Title 18, United States Code, Section 2703(g), this Application and Affidavit for search warrants seeks authorization to require Apple, and their agents and employees, to assist Agents in the execution of this warrant. Once issued, the search warrant will be presented to Apple with direction that they identify the accounts described in Attachment A to this Affidavit, as well as other subscriber and log records associated with the accounts, as set forth in Section I of Attachment B to this Affidavit.

60. The search warrant will direct Apple to create an exact copy of the specified account and records.

61. I and/or other law enforcement personnel will thereafter review the copy of the electronically stored data and identify from among that content those items that come within the items identified in Section II to Attachment B for seizure.

62. Analyzing the data contained in the forensic copy may require special technical skills, equipment, and software. It could also be very time-consuming. Searching by keywords, for example, can yield thousands of "hits," each of which must then be reviewed in context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. Keywords used originally need to be modified continuously, based on interim results. Certain file formats, moreover, do not lend themselves to keyword searches, as keywords, search text, and many common email, database and spreadsheet applications do not store data as searchable text. The data may be saved, instead, in proprietary non-text format. And, as the volume of storage allotted by service providers increases, the time it takes to properly analyze recovered data increases, as well. Consistent with the foregoing, searching the recovered data for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months. All forensic analysis of the data will employ only those search protocols and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

methodologies reasonably designed to identify and seize the items identified in Section II of Attachment B to the warrant.

63. Based on my experience and training, and the experience and training of other agents with whom I have communicated, it is necessary to review and seize a variety of e-mail communications, chat logs, and documents, that identify any users of the subject account and e-mails sent or received in temporal proximity to incriminating e-mails that provide context to the incriminating communications.

CONCLUSION

64. Based on the foregoing, I respectfully request that the Court issue the proposed search warrant. Pursuant to 18 U.S.C. § 2703(g), the government will execute the warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records and data, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night. Accordingly, by this Affidavit and Warrant, I seek authority for the government to search all of the items specified in Section I of Attachment B (attached hereto and incorporated by reference herein) to the Warrant, and specifically to seize all of the data, documents and records that are identified in Section II of Attachment B.

65. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

66. I further request, pursuant to 18 U.S.C. § 3103a(b) and Federal Rule of Criminal Procedure 41(f)(3), that the Court authorize the officer executing the warrant to delay notice until 90 days after the collection authorized by the warrant have been completed. This delay is justified because there is reasonable cause to believe that providing immediate notification of the warrant may have an adverse result, as defined in 18 U.S.C. § 2705. Providing immediate notice to the person using the SUBJECT ACCOUNT would seriously jeopardize the ongoing investigation, as such a disclosure would give that person an opportunity to destroy evidence, change patterns of behavior, notify confederates, and flee from prosecution. *See* 18 U.S.C. § 3103a(b)(1). There is

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

reasonable necessity for the use of the technique described above, for the reasons set forth above. *See* 18 U.S.C. § 3103a(b)(2). Additionally, if necessary, I may request that the Court, upon a showing of good cause, order a further delay of the time permitted to serve notice, if necessary to protect the safety of any individual, avoid flight or destruction of evidence, and ensure that the investigation is not jeopardized prior to its completion.

67. I further request that the Court order that all papers in support of this application, including the Affidavit and Search Warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

SHAWNA MCCANN, Affiant
Special Agent, FBI

The above-named agent provided a sworn statement attesting to the truth of the foregoing affidavit by telephone on this 14th day of May, 2020.

MARY ALICE THEILER
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970